Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1.   (Currently Amended) A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application; a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and used by the security manager for controlling access of the applicationto functions through the application interface the method comprising:

downloading into the apparatus an object containing access permissions and other permission information to be associated with policy contained in the downloaded object as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions;

verifying the object; and

installing the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

2.   (Previously Presented) A method according to claim 1, wherein the object is verified by checking a certificate chain of the object.

3.   (Previously Presented) A method according to claim 1-further comprising verifying that a policy of the function allows updates.

4.   (Previously Presented) A method according claim 1, further comprising installing a library comprising new routines and/or new functions to be called by an application or another library stored in the apparatus to enable access of functions through the application interface.

5.　(Previously Presented) A method according to claim 4, wherein the new routines and/or new functions can access existing functions through the library.

6.　(Previously Presented) A method according to claim 5, wherein the security manger, when accessing functions, recursively checks the permissions of the application interfaces and libraries in a linked chain related to the called functions.

7.　(Previously Presented) A method according to claim 1, further comprising installing a new function so that the new function can access existing functions through the application interface.

8.　(Previously Presented) A method according to claim 7, wherein the new functions can access existing functions through a library.

9.　(Previously Presented) A method according claim 1, wherein the access permissions are contained in a policy file.

10.　(Previously Presented) A method according to claim 9, wherein the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

11.　(Previously Presented) A method according to claim 9, wherein the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

12.　(Previously Presented) A method according to claim 11, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

13.   (Previously Presented) A method according to claim 10, wherein the policy file has a structure including logical expressions.

14.   (Currently Amended) A method of providing a dynamic security management in an apparatus, the apparatus comprising: a platform for running an application; a security manager for handling access of the application to functions existing in the apparatus; an application interface between the platform and the application; a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface, the method comprising:

storing the access permissions in a security policy; ~~and~~

downloading into the apparatus an object containing additional access permissions and other permission information to be associated with policy contained in the downloaded object as well as the access permissions in the security policy, wherein the permissions are applicable to at least one function and the object includes new routines and/or new functions; and

providing the security policy with a hierarchical structure including the access permissions in the security policy and the object containing additional access permissions and other permission information so that the object enhances the application interface with the new routines and/or new functions.

15.   (Previously Presented) A method according to claim 14, wherein the security policy has a structure linking access levels of existing functions with a domain associated with the downloaded object.

16.   (Previously Presented) A method according to claim 15, wherein the security policy has a structure linking access levels of existing functions with information contained in a certificate chain.

17.   (Previously Presented) A method according to claim 16, wherein the

information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

18.   (Currently Amended) An apparatus with dynamic security management comprising:

a platform for running an application;

a security manager for handling access of the application to functions existing in the apparatus;

an application interface between the platform and the application;

a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface wherein the apparatus is configured to download an object containing access permissions and other permission information to be associated with policy contained in the downloaded objects as well as access permissions already existing in the apparatus, wherein the permissions are applicable to at least one function, the object comprising new routines and/or new functions; to verify the object; and to install the access permissions together with the existing permissions, the object enhancing the application interface with the new routines and/or new functions.

19.   (Previously Presented) An apparatus according to claim 18, wherein the security manager is configured to verify the object by checking a certificate chain of the object.

20.   (Previously Presented) An apparatus according to claim 18 wherein the security manager is configured to verify that a policy of the function allows updates.

21.   (Currently Amended) An apparatus according to claim 18, wherein the apparatus is configured to install a library [[(12)]] comprising new routines and/or new functions to be called by an application or another library stored in the apparatus to enable

access of functions through the application interface.

22. (Previously Presented) An apparatus according to claim 21, wherein the new routines and/or new functions can access existing functions through the library.

23. (Previously Presented) An apparatus according to claim 22, wherein the security manger, when accessing functions, is configured to recursively check the permissions of the application interfaces and libraries in a linked chain related to the called functions.

24. (Previously Presented) An apparatus according claim 18, wherein the apparatus is configured to install a new function so that the new function can access existing functions through the application interface.

25. (Previously Presented) An apparatus according to claim 24, wherein the new functions can access existing functions through a library.

26. (Previously Presented) An apparatus according to claim 18, wherein the access permissions are contained in a policy file.

27. (Previously Presented) An apparatus according to claim 26, Previously Presented wherein the policy file has a structure linking access levels of existing functions with a domain associated with the downloaded object.

28. (Previously Presented) An apparatus according to claim 26, wherein the policy file has a structure linking access levels of existing functions with information contained in a certificate chain.

29. (Previously Presented) An apparatus according to claim 28, wherein the information includes a signature of the end entity certificate, a signature of an intermediate

certificate, or specific level information (level OID).

30.   (Previously Presented) An apparatus according to claim 28, wherein the policy file has a structure including logical expressions.

31.   (Currently Amended) An apparatus for providing a dynamic security management comprising:

a platform for running an application;

a security manager for handling access of the application to functions existing in the apparatus;

an application interface between the platform and the application;

a set of access permissions stored in the apparatus and used by the security manager for controlling access of the application to functions through the application interface, wherein the apparatus is configured to store the access permissions in a security policy; and provide the security policy with a hierarchical structure, wherein the apparatus is configured to download an object containing additional access permissions to be associated with policy contained in the downloaded objects as well as access permissions already existing in teh apparatus, wherein the permissions are applicable to at least one function, said object comprising new routines and/or new functions; to verify the object; and to install the access permissions together with the existing permissions; said object enhancing the application interface with the new routines and/or new functions.

32.   (Previously Presented) An apparatus according to claim 31, wherein the security policy has a structure linking access levels of existing functions with a domain associated with the downloaded object.

33.   (Previously Presented) An apparatus according to claim 32, wherein the security policy has a structure linking access levels of existing functions with information contained in a certificate chain.

34. (Previously Presented) An apparatus according to claim 33, wherein the information includes a signature of the end entity certificate, a signature of an intermediate certificate, or specific level information (level OID).

35. (Previously Presented) An apparatus according to claim 18, wherein the apparatus is a portable telephone, a pager, a communicator, a smart phone, or an electronic organiser.